August 23, 2013
HUFF POST TECH

Gerry Smith
Gerald.Smith@huffingtonpost.com

FBI Agent: We've Dismantled The Leaders Of Anonymous

Posted: 08/21/2013 11:28 am EDT | Updated: 08/22/2013 11:42 pm EDT

The hacker collective Anonymous has not produced as many high-profile cyber attacks as it once did, a drop-off that can be directly attributed to the arrests of the group's core members, an FBI official told The Huffington Post this week.

Starting in late 2010, Anonymous captured worldwide attention through a series of attacks against U.S. companies and government agencies, stealing data and defacing or crashing websites.

But the arrests last year of five members of Lulz Security, an influential splinter group of hackers, had a "huge deterrent effect" on Anonymous by creating an "added layer of distrust" within the hacking group, according to Austin P. Berglas, assistant special agent in charge of the FBI's cyber division in New York.

“All of these guys [arrested] were major players in the Anonymous movement, and a lot of people looked to them just because of what they did,” Berglas said in an interview with HuffPost.

The 2012 arrests relied on the help of a key informant, Hector Monsegur, aka "Sabu," who was caught and then cooperated with the FBI. The fear that one of their own could turn them in has sowed distrust within the hacking collective, according to Berglas.

"The movement is still there, and they're still yacking on Twitter and posting things, but you don't hear about these guys coming forward with those large breaches," he said. "It's just not happening, and that's because of the dismantlement of the largest players."

Gabriella Coleman, a professor at McGill University who studies Anonymous, said there was "no doubt" the arrests dealt a major blow to "a central node of activity" within the group. But Anonymous is still very much alive, she said.

"They could easily emerge again as a force to contend with," she told HuffPost in an email.

The arrests of members of Anonymous last year were among several highlights to come out of the FBI's cyber division in New York. (The five core members of Lulz Security have pleaded guilty.) In another case, the FBI in New York led an investigation that resulted in the arrests earlier this year of three alleged operators of the Gozi virus, which infected at least 1 million computers and stole millions of dollars from banks around the world.

A former Army captain, 41-year-old Berglas leads the FBI's cyber division in New York, one of the busiest of the FBI's 56 field offices. His office overlooks the skyline of lower Manhattan, the center of the financial world and a frequent target of hackers. Last month, a Russian man was charged with breaking into the servers of the Nasdaq stock exchange and deleting, changing and stealing data.

The cyber division in New York is divided into five teams of investigators. One unit is tasked with getting digital evidence off cell phones, cameras, computers and tablets to support investigations into a wide range cases, from organized crime to computer hacking to child pornography. Berglas said the investigators for the Computer Analysis Response Team have become increasingly adept at breaking encryption methods used by suspects to conceal the contents of computer files.

Austin P. Berglas, FBI assistant special agent.

The other four teams divide their attention to cybercrime based on the hackers' country of origin. Since most hackers attack U.S. computers from overseas, the FBI often works with law enforcement in other countries, Berglas said. Sometimes, investigators find evidence of hackers from several different countries inside the network of a single U.S. company.

"We call it the dirty pond environment," he said. "You think it might just be one actor responsible for the intrusion, and once you get in and start looking at the company there's remnants of a whole host of actors -- from week-old activity to multiple years they've been inside some companies and they just don’t know about it."

Cybercriminals have a variety of motives, but their methods are often the same. Most break into computer systems by tricking people to click on malicious links in emails that appear to come from trusted sources, a technique known as "spear phishing," Berglas said.

"It’s the number one most common intrusion vector we see in any type of attack,” Berglas said. "Major financial companies spend millions and millions of dollars on security, and all [hackers] have to do is get someone with credentials to click on a spear-phishing site and that’s how they get in.”

Cybercriminals have become adept at hiding their IP addresses -- the string of numbers assigned to individual computers -- to disguise their

locations from law enforcement. But eventually, even the most skilled hackers get sloppy, Berglas said.

Hector Monsegur, aka "Sabu," the FBI informant whose cooperation led to the arrests of LulzSec last year, left his IP address exposed. The error allowed investigators to track his location to an apartment in Manhattan's Lower East Side and eventually led to his arrest.

It's that type of misstep that the FBI is looking for.

"It's easy to sit behind a computer and think you're anonymous and do these illegal types of activity, whether it's hacking into a company or trading child pornography or buying and selling stolen identities," he said. "But it's just a matter of time before these criminals make mistakes and we capture them. All it takes is just one time."